荣耀平板t1823l优享版具有荣耀系列产品的共性，但市场上此款产品的刷机包并不常见，本文以这款产品为例谈一下手机root、boot-loader解锁及xposed安装过程。

# 1 root设备时经常出现的问题

【问题1】使用最新的android sdk manager下载的adb工具连接到t1823l设备时，会出现adb server与client不匹配的现象，但通过奇兔刷机助手中的低版本adb工具可以正常连接，可见前后两者adb工具版本不同。输入adb version查看版本，前者为：Android Debug Bridge version 1.0.39 Revision 3db08f2c6889-android，后者为：Android Debug Bridge version 1.0.31。

【问题2】输入adb root时，提升”adbd cannot run as root in production builds”，其原因为手机未root充分，解决方案为：安装“超级adbd.apk”软件→授予其root权限→勾选“启用超级adbd”选项。再次输入adb root，提示”adbd is already running as root”，此时直接进入adb shell，发现默认账户即root。



【附件】超级adbd.apk



【问题3】adb remount提示read-only file system，在执行adb reboot后，可执行成功，但过几秒钟/system会自动变成只读，具体原因可能和fastboot未解锁有关。

mount -o remount,rw /dev/block/bootdevice/by-name/system /system

# 2 安装使用xposed

# 安装最新版本的xposed

adb.exe install -r "de.robv.android.xposed.installer\_v33\_36570c.apk"

# 在宿主机解压缩xposed apk包，将XposedBridge.jar和app\_process复制到虚拟机

adb.exe push de.robv.android.xposed.installer\_v33\_36570c\assets\XposedBridge.jar /data/data/de.robv.android.xposed.installer/bin

# 由于remount后在较短时间内，/system会自动变成read-only，因此app\_process覆盖操作为连贯动作

adb shell "mount -o remount,rw /dev/block/bootdevice/by-name/system /system"

adb push de.robv.android.xposed.installer\_v33\_36570c\assets\arm\app\_process\_xposed\_sdk16 /system/bin/app\_process

adb shell "chmod 06755 /system/bin/app\_process"

adb shell "ls -l /system/bin/app\_process"

# “无论是通过修改出厂镜像来创建定制系统镜像，还是通过源码编译你自己的镜像，你都必须将其刷入系统分区来使之生效”——《Android安全攻防权威指南》，如

*fastboot flash system custom-system.img*

# 3 尝试刷入修改后的system.img

# 在宿主机上执行make\_ext4fs导出分区到img文件

make\_ext4fs -l 1740M -s -a system -v system\_modified\_170805.img /system

# 下载img镜像到本地

adb.exe pull /mnt/shell/emulated/system\_modified\_170805.img

# 一般通过make\_ext4fs导出的img为yaffs2格式，因此需要转换成ext4格式，**但后续就会发现这一步是多余的**

simg2img\_win-master\simg2img.exe system\_modified\_170805.img system\_modified\_170805\_ext4.img

# 尝试使用fastboot刷入rom，但提示无法分配空间

*load\_file: could not allocate XXXX bytes*

*error: cannot load ‘system.img’*

# 原因是常规fastboot无法处理Android 5.1固件的system.img大小

# 尝试使用mfastboot

mfastboot.exe flash system system\_modified\_170805\_ext4.img

# 执行时报非法操作，并提示在magi头部存在无效的稀疏文件格式

*target max-download-size: 254MB*

*Invalid sparse file format at header magi*

# 再尝试使用未经过simg2img格式化的原始镜像

mfastboot flash system .\system\_modified\_170805.img

# 运行一段时间后报错

*target max-download-size: 254MB*

*Sparse-Flash is enabled!*

*sending sparse 'system' (259720 KB)...*

*OKAY [ 11.165s]*

*writing 'system'...*

*FAILED (****remote: Command not allowed****)*

*finished. total time: 11.185s*

# 出现这种问题是由于bootloader被锁，需要进行解锁

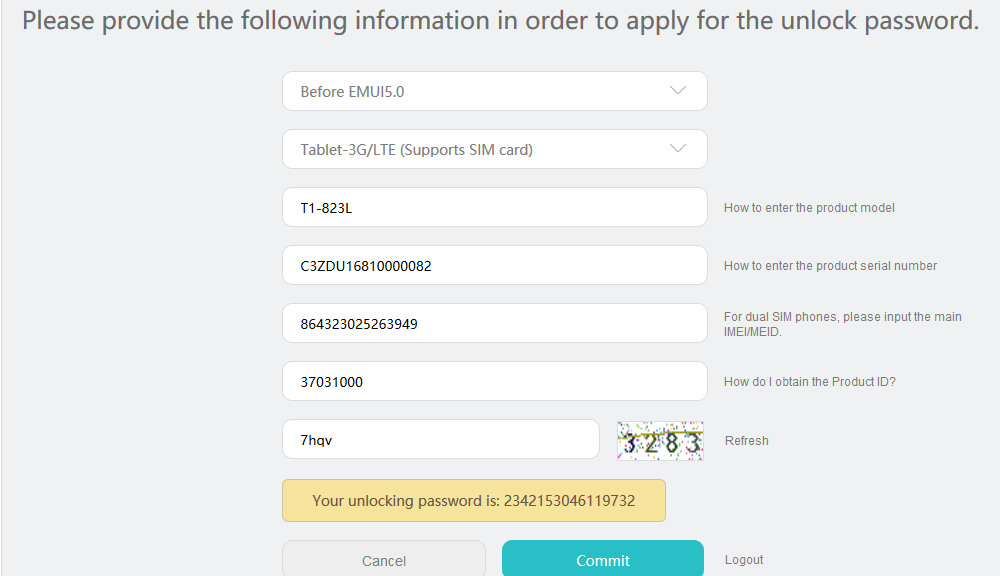
# 4 Bootloader解锁过程

一、访问：

https://redirect.viglink.com/?format=go&jsonp=vglnk\_150194893516421&key=f0a7f91912ae2b52e0700f73990eb321&libId=j5zgmckq01000n4o000DAbxredfxa&loc=https%3A%2F%2Fforum.xda-developers.com%2Fhonor-5x%2Fhow-to%2Fhow-to-unlo-t3306961&v=1&out=http%3A%2F%2Femui.huawei.com%2Fen%2Fplugin.php%3Fid%3Dhwdownload%26mod%3Dlist&ref=https%3A%2F%2Fcn.bing.com%2F&title=How%20to%20unlock%20the%20honor%205X%20bootloader%20%7C%20Honor%205X&txt=http%3A%2F%2Femui.huawei.com%2Fen%2Fplugin.php...nload%26amp%3Bmod%3Dlist

二、注册华为ID，登陆系统，输入终端信息，获取解锁密码

【注意】可以根据输入框右侧的提示找到获取这些数据的方法



三、在fastboot模式下查看LOCK状态

# 将平板重启到fastboot模式

adb reboot bootloader

# 查看root和bootloader锁状态，发现bootloader确实未解锁

fastboot oem get-bootinfo

# 可看到如下信息

*(bootloader) Bootloader Lock State: LOCKED*

*(bootloader) Root State: ROOT*

# 执行解锁命令，参数为前面获取到的解锁密码

fastboot oem unlock 2342153046119732

# 提示如下内容

*...*

*(bootloader) Unlock success , the device will reboot and factory reset*

*OKAY [ 0.038s]*

*finished. total time: 0.039s*

# 系统自动重启，并格式化/data分区，此后系统自动重置

# 重新进入bootloader模式，查看解锁状态为UNLOCKED

adb reboot bootloader

# 重新刷入system

mfastboot flash system system\_modified\_170805.img

# 提示内容无报错，刷入成功

*target max-download-size: 254MB*

*Sparse-Flash is enabled!*

*sending sparse 'system' (259720 KB)...*

*OKAY [ 11.360s]*

*writing 'system'...*

*OKAY [ 11.906s]*

*sending sparse 'system' (257713 KB)...*

*OKAY [ 10.572s]*

*writing 'system'...*

*OKAY [ 11.485s]*

*sending sparse 'system' (257710 KB)...*

*OKAY [ 10.829s]*

*writing 'system'...*

*OKAY [ 11.500s]*

*sending sparse 'system' (259269 KB)...*

*OKAY [ 11.203s]*

*writing 'system'...*

*OKAY [ 11.580s]*

*sending sparse 'system' (260093 KB)...*

【注意】Bootloader解锁后root权限丢失，需要重新进行root操作